



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

Address: COMMISSIONER FOR PATENTS

P.O. Box 1450

Alexandria, Virginia 22313-1450

www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/706,871	11/12/2003	Nicholas Stamos	3602.1000-002	6738
21005 7590 05/09/2008 HAMILTON, BROOK, SMITH & REYNOLDS, P.C. 530 VIRGINIA ROAD P.O. BOX 9133 CONCORD, MA 01742-9133				
EXAMINER				
MURDOUGH, JOSHUA A				
ART UNIT		PAPER NUMBER		
3621				
MAIL DATE		DELIVERY MODE		
05/09/2008		PAPER		

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

# Office Action Summary

**Application No.**

10/706,871

**Applicant(s)**

STAMOS ET AL.

**Examiner**

JOSHUA MURDOUGH

**Art Unit**

3621

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 11 February 2008.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-22 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-22 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO/SD/US)
- Paper No(s)/Mail Date 3/26/2008
- 4) ☐ Interview Summary (PTO-413)
- Paper No(s)/Mail Date \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_

**DETAILED ACTION**

***Acknowledgements***

1. Claims 1-22 are pending.

***Continued Examination Under 37 C.F.R. §1.114***

2. A request for continued examination under 37 C.F.R. §1.114, including the fee set forth in 37 C.F.R. §1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 C.F.R. §1.114, and the fee set forth in 37 C.F.R. §1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 C.F.R. §1.114. Applicant's submission filed on 11 February 2008 has been entered.

***Specification***

3. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 C.F.R. §1.75(d)(1) and MPEP §608.01(o). Correction of the following is required:
4. "IRP intercept" as recited in claims 4 and 15.

***Claim Objections***

5. Claims 13-22 are objected to because of the following informalities: Claim 12 is directed toward a system, but claims 13-22 claim it as an apparatus. Appropriate correction is required.

***Claim Rejections - 35 USC §112 2<sup>nd</sup> Paragraph***

6. The following is a quotation of the second paragraph of 35 U.S.C. §112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claims 4 and 15 are rejected under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

- a. In claims 4 and 15, the phrase “IRP intercept” is indefinite. It is the Examiner’s position that one of ordinary skill in the art would not recognize this term as old and well known. Applicants’ specification does not define it in a manner that clearly and distinctly explains the term. Therefore, it is considered indefinite until such time that Applicants show a distinct explanation from the specification, or if Applicants state clearly on the record that it is old and well known in the art, as well as, providing a reference in support of the statement, in order to have the rejection withdrawn.
- b. For purposes of applying the prior art in accordance with MPEP §2173.06, an IRP intercept has been interpreted to be an interrupt. The Examiner has applied this interpretation to the claims in order to provide compact prosecution of the application and to prevent piecemeal examination.

***Claim Rejections - 35 USC § 102***

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

Art Unit: 3621

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

9. Claims 1-5, 7, 8, 10-13, 15, 16, 18, 19, 21, and 22, as best understood by the Examiner, are rejected under 35 U.S.C. 102(e) as being anticipated by Carter et al. (US 2003/0051026) ("Carter").

10. As to claim 1, Carter shows:

An agent process for controlling access to digital assets in a

network of data processing devices comprising:

defining a security perimeter **114** that includes two or more data processing devices

(protected servers, figure 1);

defining one or more policy violation predicates (Paragraphs 0775-0783), that are

asserted upon an occurrence of a possible risk of use of a digital asset by an end

user outside of the security perimeter (Paragraphs 0787-0791 and tables included

within);

sensing atomic level digital asset access events (listed after paragraph 0787),

the sensing step located within an operating system kernel (Paragraph 0147) within an

end user client device (workstation, Figure 1), at a point of authorized access

(through switch controlled by the Network Surveillance and Security System,

"NSSS" **18**) to the digital asset (located on a protected server within group **114**)

by the end user;

aggregating multiple atomic level events to determine a combined event (Paragraph

0435); and

asserting a policy violation predicate upon an occurrence of a combined event that violates a predefined digital asset usage policy that indicates a risk of use of the digital asset outside (inherent because the workstation is outside of the secure switch) of the security perimeter (Paragraph 0435).

11. As to claim 12, Carter shows:

A system for controlling access to digital assets in a network of data processing devices comprising:

a digital asset usage policy server **18**, for storing one or more digital asset usage policies (Paragraphs 0787-0791 and tables included within) to be applied to a security perimeter **114**, the security perimeter comprising two or more data processing devices (protected servers, figure 1);

an atomic level data processing asset access event sensor (things sensed listed after paragraph 0787), the sensor located within an operating system kernel (Paragraph 0147) within an end user client device (workstation, Figure 1), to sense atomic level events at a point of authorized access (through switch controlled by the Network Surveillance and Security System, "NSSS" **18**) by the end user device to one or more digital assets;

an atomic level event aggregator (Paragraph 0435), to determine the occurrence of an aggregate event that comprises more than one atomic level asset access event; and a policy violation detector, for determining if a combination of combined events has occurred that violates a predefined digital asset usage policy (Paragraph 0435) that indicates a risk of use of a digital asset outside the security perimeter (Paragraph 0224).

12. As to claims 2 and 13, Carter further shows:  
  
the step of asserting the policy violation predicate is implemented in an operating system  
  
kernel of the client user device (element 1018, figure 10) .
13. As to claim 3, Carter further shows:  
  
preventing a user from accessing the digital asset if the policy predicate indicates  
  
a violated policy (Paragraph 1040).
14. As to claims 4 and 15, Carter further shows:  
  
the preventing step includes an IRP intercept (Paragraph 0147, interrupt handler within  
  
the kernel).
15. As to claims 5 and 16, Carter further shows:  
  
the combined event is a time sequence of multiple atomic level events (Paragraph 0224).
16. As to claims 7 and 18, Carter further shows:  
  
asserting multiple policy violation predicates (Paragraph 0435) prior to indicating a risk  
  
of use of the digital asset outside of the security perimeter (Paragraph 0224).
17. As to claims 8 and 19, Carter further shows:  
  
operates independently of application software (It is within the kernel, which is part of  
  
the Operating System, not the application software).
18. As to claims 10 and 21, Carter further shows:

the sensors, aggregators, and asserting steps operate in real time (Abstract, real time updating of the knowledge base requires that the sensors, aggregators, and asserting of predicates also operate in real time).

19. As to claims 11 and 22, Carter further shows:  
determining the identity of a particular file in the asset access event (Paragraph 0162, In order to access the remote file through the local file, the system needs to determine the identity of the remote file.).
20. As to claim 14, Carter further shows  
the policy violation detector determines a violated policy type (Shown as classes of violations in the table following paragraph 0787).

***Claim Rejections - 35 USC § 103***

21. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

22. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Carter in view of Danieli (US 6,510,513).
23. As to claim 9, Carter shows all of the elements of claim 1, but does not directly show the notification of the user that they have violated a policy. Danieli teaches "alerting a user of the



client computer of the inappropriate use" (see claim 14). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the invention of Carter by adding the teachings of Danieli to make it known to the user that there was a violation, because the notification allows the user to know they have done something the system believes they should not, enabling them to justify their actions to a responsible party and possibly get the policy changed, if their actions were justified.

24. Claims 6, 17, and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Carter in view of Admitted Prior Art.

25. As to claims 6, 17, and 20, Carter shows all of the elements except for the ability of the user to document their reason for the policy violation. It is now considered admitted prior art that documenting the reason for an access is old and well known in the art. (See statement on Official Notice in paragraph 37 below.) It therefore would have been obvious to one of ordinary skill in the art at the time of the invention to modify the invention of Carter to incorporate this functionality. The ability to document the reason at the time of the occurrence would provide for a record of what was done and why, saving the effort of finding the appropriate person to notify.

26. Claims 1-5, 7, 8, 10-13, 15, 16, 18, 19, 21, and 22, as best understood by the Examiner, are *alternatively* rejected under 35 USC 103(a) by Carter in view of Danieli.

27. As to claims 1 and 12, the Examiner's primary position is that it is inherent in Carter that the digital asset is used outside of the perimeter because the workstation using the asset is outside of the secure switch (Figure 1). However if not inherent, it is the Examiner's alternate position that

Art Unit: 3621

Danieli clearly shows the process of securing a digital asset outside of the perimeter (Figure 6). Therefore, if not inherent, it would have been obvious to one of ordinary skill in the art at the time of the invention to have modified the teachings of Carter to include the external security method of Danieli in order to extend the range of control over the digital assets past the security perimeter.

28. As to claims 2 and 13, Carter further shows:

the step of asserting the policy violation predicate is implemented in an operating system kernel of the client user device (element 1018, figure 10) .

29. As to claim 3, Carter further shows:

preventing a user from accessing the digital asset if the policy predicate indicates a violated policy (Paragraph 1040).

30. As to claims 4 and 15, Carter further shows:

the preventing step includes an IRP intercept (Paragraph 0147, interrupt handler within the kernel).

31. As to claims 5 and 16, Carter further shows:

the combined event is a time sequence of multiple atomic level events (Paragraph 0224).

32. As to claims 7 and 18, Carter further shows:

asserting multiple policy violation predicates (Paragraph 0435) prior to indicating a risk of use of the digital asset outside of the security perimeter (Paragraph 0224).

33. As to claims 8 and 19, Carter further shows:  
operates independently of application software (It is within the kernel, which is part of the Operating System, not the application software).
34. As to claims 10 and 21, Carter further shows:  
the sensors, aggregators, and asserting steps operate in real time (Abstract, real time updating of the knowledge base requires that the sensors, aggregators, and asserting of predicates also operate in real time).
35. As to claims 11 and 22, Carter further shows:  
determining the identity of a particular file in the asset access event (Paragraph 0162, In order to access the remote file through the local file, the system needs to determine the identity of the remote file.).
36. As to claim 14, Carter further shows  
the policy violation detector determines a violated policy type (Shown as classes of violations in the table following paragraph 0787).

***Claim Interpretations***

37. Since Applicants did not seasonably traverse the Official Notice statement as stated in the previous Office Action, mailed 9 November 2007, (Page 6) the Official Notice statement are taken to be admitted prior art. See MPEP §2144.03

38. Claims 12-22 are understood to be apparatus claims. As such, they are subject to interpretation as outlined by MPEP § 2114, wherein it says, “While features of an apparatus may be recited either structurally or functionally, claims directed to an apparatus must be distinguished from the prior art in terms of structure rather than function” and “[A]pparatus claims cover what a device is, not what a device does.” While the Examiner has cited references for the functional limitations that do not require an alteration of the structure for purposes of compact prosecution, it is his principal position that these elements do not need to be shown in order to show anticipation. It is suggested that the claims be amended to clearly show the structural elements to prevent issues associated with this type of interpretation.

### ***Double Patenting***

39. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the “right to exclude” granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225

Art Unit: 3621

USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

40. A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

41. Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

42. Claims 1-22 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-16 of U.S. Patent No. 7,100,047. Although the conflicting claims are not identical, they are not patentably distinct from each other because the primary subject matter is the same, e.g. multi-device security perimeter, sensing from the kernel, and multiple atomic events being aggregated into a combined event.

43. Furthermore, there is no indication why the claims of the instant application could not have been included in the application that lead to the '047 patent.

### ***Conclusion***

44. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

45. Holden (US 5,692,124) shows the control of data flow from high security areas of a network to those with lower security.
46. Teal (US 2003/0120935) shows kernel-based network security infrastructure.
47. Any inquiry concerning this communication or earlier communications from the examiner should be directed to JOSHUA MURDOUGH whose telephone number is (571)270-3270. The examiner can normally be reached on Monday - Thursday, 7:00 a.m. - 5:00 p.m.
48. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Fischer can be reached on (571) 272-6779. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.
49. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

J. M.  
Examiner, Art Unit 3621

/ANDREW J. FISCHER/  
Supervisory Patent Examiner, Art Unit 3621